**U.S. Secret Service**

**Testimony of Mr. James A. Savage, Jr.**
**Deputy Special Agent in Charge-Financial Crimes Division**

**Before**

**The Senate Committee on the Judiciary**
**Subcommittee on Technology, Terrorism and Government Information**

**July 25, 2001**

Madam Chairman, members of the subcommittee, thank you for the opportunity to address the subcommittee regarding federal law enforcement efforts in combating cyber crime to protect our nation's infrastructures, and particularly the efforts of the Secret Service in this regard. I am particularly pleased to be here with my colleagues and partners in fighting cyber crime from the Federal Bureau of Investigation and the General Services Administration.

As you know, the Secret Service was created in 1865 to address the burgeoning problem of counterfeit currency. At that time, it was estimated that approximately one third of all currency in circulation was counterfeit and the government recognized the urgent need to address this issue in order to maintain the public's confidence in the U.S. currency. In effect, the Secret Service was engaged in an effort to protect a critical governmental function long before the popular notion of critical infrastructure protection emerged.

Today, the Secret Service continues to suppress counterfeit currency as part of its traditional role but also now includes fighting cyber crime as part of our core mission to protect the integrity of this nation's financial payment systems. Over time, modes and methods of payment have evolved and so has our mission. Computers and other "chip" devices are now the facilitators of criminal activity or the target of such. The perpetrators involved in the exploitation of such technology range from traditional fraud artists to violent criminals – all of whom recognize new opportunities and anonymous methods to expand and diversify their criminal portfolio.

In this era of change, one constant that remains is our close working relationship with the banking and finance sector. Our history of cooperation with the industry is a result of our unique responsibilities as a law enforcement bureau of the Department of the Treasury. We believe that protection of the banking and financial infrastructure is our "core competency" area.

Madam Chairman, there is no shortage of information, testimony, or anecdotal evidence regarding the nature and variety of cyber-based threats to our banking and financial infrastructures and the need to create effective solutions. There is, however, a scarcity of

information regarding successful models to combat such crime in today's high tech environment. That is where the Secret Service can make a significant contribution to today's and future discussions of successful law enforcement efforts to combat cyber crime which play an important role in critical infrastructure protection.

The Secret Service has found a highly effective formula for combating high tech crime – a formula that has been successfully developed by our New York Electronic Crimes Task Force. While the Secret Service leads this innovative effort, we do not control or dominate the participants and the investigative agenda of the task force. Rather, the task force provides a productive framework and collaborative crime-fighting environment in which the resources of its participants can be combined to effectively and efficiently make a significant impact on electronic crimes. Other law enforcement agencies bring additional criminal enforcement jurisdiction and resources to the task force while representatives from private industry, such as telecommunications providers, for instance, bring a wealth of technical expertise.

Although based in New York City, the task force provides assistance and conducts investigations, which span the country and often lead overseas, harnessing disparate repositories of resources and expertise from the academic, private and government sectors. It is not uncommon for the New York Task Force to receive requests for assistance directly from foreign law enforcement representatives based upon its reputation for responsiveness and as a center of excellence. The result is a significant impact domestically, and occasionally abroad, as well.

Within this New York model, established in 1995, there are 50 different federal, state and local law enforcement agencies represented as well as prosecutors, academic leaders and over 100 different private sector corporations. The wealth of expertise and resources that reside in this task force coupled with unprecedented information sharing yields a highly mobile and responsive machine. In task force investigations, local law enforcement officers hold supervisory positions and representatives from other agencies regularly assume the role of lead investigator. These investigations encompass a wide range of computer-based criminal activity, involving e-commerce frauds, intellectual property violations, telecommunications fraud, and a wide variety of computer intrusion crimes, which affect a variety of infrastructures.

Since 1995, the task force has charged over 800 individuals with electronic crimes valued at more than $425 million. It has trained over 10,000 law enforcement personnel, prosecutors, and private industry representatives in the criminal abuses of technology and how to prevent them. We view the New York Electronic Crimes Task Force as the model for the partnership approach that we hope to employ in additional venues around the country in the very near future.

An important component in our investigative response to cyber crime and critical infrastructure protection is the Electronic Crimes Special Agent Program (ECSAP). This program is comprised of approximately 175 special agents who have received extensive training in forensic identification, preservation, and retrieval of electronically stored

evidence. Special Agents entering the program receive specialized training in all areas of electronic crimes, with particular emphasis on computer intrusions and forensics. ECSAP agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence, including computers, personal data assistants, telecommunications devices, electronic organizers, scanners, and other electronic paraphernalia. ECSAP agents understand that not only do they have an investigative role, and that they can also help protect components of our critical infrastructure by providing their substantive insights regarding potential vulnerabilities and exploits which the Secret Service discovers during an investigation.

As a specific example, in early August we will be meeting with representatives of a major financial group, which is in the process of developing its own computer forensic capability to bolster its defenses against internal and external computer based frauds and attacks. We hope to share with this prominent corporation the lessons we have learned in establishing and maintaining our ECSAP computer forensics program as well as explore areas for joint endeavors in the future.

The Secret Service ECSAP program relies on the 4 year-old, Treasury-wide Computer Investigative Specialist (CIS) initiative. All four Treasury law enforcement bureaus – the Internal Revenue Service, Bureau of Alcohol, Tobacco and Firearms, U.S. Customs Service, and the U.S. Secret Service -- participate and receive training and equipment under this program.

All four Treasury bureaus also jointly participate in curriculum development and review, equipment design and distribution of training assets. As a result, financial savings by all Treasury bureaus are realized due to economies of scale. Additionally, agents from different bureaus can work together in the field in an operational capacity due to the compatibility of the equipment and training. In the end, the criminal element suffers and the taxpayer benefits.

The Secret Service works cooperatively with other federal law enforcement and Department of Defense agencies in this work, to include the FBI and NIPC. No single agency or entity can prevent cybercrime or protect the critical infrastructure alone, so Secret Service agents work collaboratively with their peers in the field to investigate crimes and overcome technical problems. I would further add, Madam Chairman, that due to the proliferation and complexity of cyber crime there is certainly no shortage of opportunity to collaborate with our other Federal partners in this regard.

Because of the recognized expertise of those in ECSAP, other law enforcement agencies regularly request training from the Secret Service or advice concerning their own computer forensics programs. These requests have come from agencies all across the country, as well as foreign countries such as Italy and Thailand. The Secret Service recognizes the need to promote international cooperation and remains proactive in the dissemination of information to law enforcement agencies, both domestically and internationally, regarding program initiatives and current financial and electronic crimes trends.

Madam Chairman, we are committed to working closely with our law enforcement counterparts worldwide in response to cyber crime threats to commerce and financial payment systems. This commitment is demonstrated by our effort to expand our overseas presence. We currently have 18 offices in foreign countries and a permanent assignment at Interpol, as well as several overseas initiatives, including a cyber crime task force in Indonesia. New offices have been opened recently in Frankfurt, Lagos, and Mexico City. The Secret Service is also considering opening new offices in Bucharest and New Dehli. Our expanded foreign presence increases our ability to become involved in foreign investigations that are of significant strategic interest.

In addition to providing law enforcement with the necessary technical training and resources, a great deal more can be accomplished in fighting cyber crime if we are able to harness additional resources that exist from the private sector and academia. The Secret Service believes there is value in sharing information during the course of our investigations with both those in the private sector and academia who are devoting substantial resources to protecting their networks and researching new solutions. On occasion the Secret Service has shared case-specific information derived from our criminal investigations after taking appropriate steps to protect privacy concerns and ensure that there are no conflicts with prosecutorial issues. I would add that there are many opportunities for the law enforcement community to share information with our private sector counterparts without fear of compromise. The Secret Service recognizes the need for a "paradigm shift" with respect to this type of information sharing between law enforcement and our private sector and academic counterparts.

Finally, law enforcement in general is not sufficiently equipped to train all those in need nor can it compete with academic institutions of higher learning in the area of research and development. However, our partnerships with industry and academia have demonstrated that this should be an integral part of the solution.

Partnership concepts are an important tool and strategy in both government and private industry to achieve greater results and efficiencies. Unfortunately, however, partnerships cannot be legislated, regulated, or stipulated. Nor can partnerships be purchased, traded or incorporated. Partnerships are built between people and organizations that recognize the value in joint collaboration toward a common end. They are fragile entities, which need to be established and maintained by all participants and built upon a foundation of trust.

The Secret Service, by virtue of the protective mission for which we are so well known, has always emphasized discretion and trust in executing our protective duties. We learned long ago that our agency needed the full support and confidence of local law enforcement and certain key elements of the private sector to create and maintain a successful and comprehensive security plan. Furthermore, we are also keenly aware that we need to maintain a trusted relationship with our protectees so that we can work with them and their staffs to maintain the delicate balance between security and personal privacy.

This predisposition towards discretion and trust naturally permeates our investigative mission where we enjoy quiet successes with our private sector partners. We have successfully investigated many significant cases with the help of our private sector partners such as network intrusions and compromises of critical information or operating systems. In such cases, even though we have technical expertise that is second to none, we still rely on our private sector counterparts to collaborate with us in identifying and preserving critical evidence to solve the case and bring the perpetrator to justice. Equally important in such cases is conducting the investigation in a manner that avoids unnecessary disruption or adverse consequences to the victim or business. With the variety of operating platforms and proprietary operating systems in the private sector, we could not accomplish these objectives without the direct support of our private sector counterparts.

I would like to highlight several significant cases that the Secret Service has investigated over the years where we have protected the U.S. financial and telecommunications systems.

In 1986, the USSS identified and prosecuted the "Legion of Doom" hacker group for compromising the 911 system in the southeast United States.

In 1989, the USSS, working with the FBI and other law enforcement entities, identified and prosecuted the "Masters of Deception" hacker group which had compromised several communications networks in the U.S. enabling the group to identify and reveal the details concerning on-going law enforcement wiretaps.

In 1994, the USSS conducted the first e-mail wiretap ever conducted on the Internet as part of a telecommunications fraud investigation.

In 1997, the USSS identified and arrested a hacker responsible for compromising a telephone network switch on the east coast, effectively disabling power and communications to the Worcester, MA. Airport. This resulted in the first prosecution of a juvenile for violation of 18 USC 1030.

In 1998, the USSS and its task force partners in New York, identified and arrested individuals who were illegally monitoring law enforcement Mobile Data Terminals.

Madam Chairman, the USSS continues to remain engaged in these types of significant investigations, which not only involve notable financial losses, but also represent the exploitation of technical vulnerabilities in and amongst interconnected computer-based systems which support our critical infrastructures. Of particular note is that such cases necessarily require a close working relationship with the private sector victim to achieve success.

In fact, in one recently completed complex investigation involving the compromise of a wireless communications carrier's network, our case agent actually specified in the

affidavit of the federal search warrant that representatives of the victim business be allowed to accompany federal agents in the search of the target residence to provide technical assistance. This is unprecedented in the law enforcement arena and underscores the level of trust we enjoy with those we have built relationships with in the private sector. It is also indicative of the complexity of many of these investigations and serves to highlight the fact that we in law enforcement must work with private industry to be an effective crime fighting force. In approving this search warrant, the court recognized that in certain cases involving extraordinarily complex systems and networks, such additional technical expertise could be a critical, and sometimes imperative, component of our investigative efforts.

I must point out, however, that such cases are usually not publicized without the express consent of the U.S. Attorney and the corporate victim because it would breach our confidential relationship and discourage the victims of electronic crimes from reporting such incidents.

Four recently concluded investigations demonstrate the breadth of cases the Secret Service is working, and provide concrete evidence of the continuing success of ECSAP. The cases include the malicious shutdown of a medical service provider's communications system, an intrusion into a telecommunication provider's network, an attack on a private investment company's trading network, and the disruption of a financial institution's complete operating system and communications network.

The first case was initiated on March 5, 2001, when a local Secret Service field office received information that a medical diagnostic service provider had suffered a catastrophic shutdown of its computer network and communications system. The company reported that they were unable to access doctor schedules, diagnostic images, patient information, and essential hospital records, which adversely affected their ability to provide care to patients and assist dependent medical facilities.

Within a matter of hours, a Secret Service ECSAP agent was able to regain control of the network by coordinating with the facility's system administrator to temporarily shutdown and reconfigure the computer system. The ECSAP agent also essentially "hacked" into the compromised system, and modified compromised password files to "lock out" the attacker. This was accomplished while maintaining control of the computer system log files containing evidence of how the intrusion had occurred.

Using this evidence, a federal search warrant was obtained for the residence of a former employee of the hospital, who had recently been terminated from his position as system administrator. Computer equipment was seized pursuant to the warrant, the suspect admitted to his involvement, and federal computer fraud charges are pending.

A case with obvious critical infrastructure implications was initiated on February 20, 2001, when two major wireless telecommunications service providers notified the New York Electronic Crimes Task Force that they had identified two hackers in different remote sites who were attacking their systems. These hackers were manipulating the

systems to obtain free long distance service, re-route numbers, add calling features, forward telephone numbers, and install software that would ensure their continued unauthorized access.

The level of access obtained by the hackers was virtually unlimited, and had they chosen to do so, they could have shut down telephone service over a large geographic area, including "911" systems, as well as service to government installations and other critical infrastructure components.

On March 20, 2001, the Secret Service simultaneously executed search warrants in New York City and Phoenix and computer equipment was seized at both locations. One suspect was arrested on federal computer fraud charges, while the other suspect was questioned and released pending a decision by the Department of Justice as to whether or not to pursue federal charges.

The third case occurred from March 9, 2000, through March 14, 2000, when a company located in New York, NY, received several Internet-based "denial of service" attacks on its servers. A "denial of service" attack occurs when a perpetrator launches malicious programs, information, codes, or commands to a target or victim computer which causes it to shut down, thereby denying access by legitimate customers to those computers. In this instance, the company was a prominent provider of electronic trading services on Wall Street.

While the attacks were still occurring, the company's CEO contacted the Secret Service's New York Electronic Crimes Task Force. The CEO identified a former employee as a suspect, based upon the fact that the attacks preyed on vulnerabilities, which would only be known to the former employee. These attacks continued through March 13, 2000, when ECSAP agents and task force members identified the attacking computer and arrested the former employee for violating Title 18, USC, Section 1030 (Computer Fraud). In a post-arrest statement, the suspect admitted that he was responsible for the denial of service attacks. As a result of the attacks, the company and its customers lost access to trading systems. Approximately $3.5 million was identified in lost trading fees, commissions, and liability as a result of the customers' inability to conduct any trading.

The last case began just last month when a financial institution notified local police who in turn notified the local office of the Secret Service, that its entire banking and communications network had been shut down. The institution reported that it was severely crippled, as it had no access to electronic data used in support of its ATMs, banking transactions, employee payroll and all other critical functions. Working with the local police and the bank's technical staff, a former employee emerged as a suspect and electronic evidence was developed that strongly indicated his involvement. During an ensuing interview with agents and police, the suspect admitted to disabling the bank's system and "hacking" an unrelated database in his attempts to exact revenge upon the bank CEO. Federal charges are pending.

Let me emphasize the Secret Service's mission in fighting cyber crime as it relates to the bigger picture of critical infrastructure protection. As previously stated, we target cyber crime as it may affect the integrity of our nation's financial payment and banking systems. As we all know, the banking and finance sector comprises a very critical infrastructure sector and one, which we have historically protected and will continue to protect. In this context, our efforts to combat cyber assaults, which target information, and communication systems, which support the financial sector, are parts of the larger and more comprehensive critical infrastructure protection scheme. The whole notion of infrastructure protection embodies an assurance and confidence in the delivery of critical functions and services that in today's world are increasingly interdependent and interconnected. To put this all in perspective, the public's confidence is lost if such delivery systems and services are unreliable, unavailable, or unpredictable regardless of the cause of the problem.

We also recognize that our unique protective responsibilities, including our duties as the lead federal agency for coordinating security at National Special Security Events, demand heightened electronic security awareness and preparation. A well-placed cyber attack against a weak technology or support infrastructure system can render an otherwise sound physical security plan vulnerable and inadequate.

To further advance our efforts in this regard, the Secret Service will soon commence a significant collaborative project with the Software Engineering Institute (SEI) at Carnegie Mellon University which has operated the Computer Emergency Response Team (CERT) Coordination Center since 1988. Jointly, the Secret Service and the SEI plan to combine expertise in developing strategies and programs to effectively address cyber threats, which may impact our protective and investigative missions.

Madam Chairman, it should also be noted that all deliberate infrastructure attacks, before they rise to such a threshold, are also cyber crimes and are likely to be dealt with initially by law enforcement personnel, both federal and local, in the course of routine business. In fact, I don't believe there is universal agreement as to when a "hack" or network intrusion rises to the threshold of an infrastructure attack and corresponding national security event but we would all probably recognize one when it reached catastrophic proportions.

Given this continuum and interplay between computer-based crimes and national security issues, the Secret Service recognizes that its role in investigating and helping to prevent computer-based attacks against the financial sector can be significant in the larger plan for the protection of our nation's critical infrastructures. When we arrest a criminal who has breached and disrupted a sensitive communications network and are able to restore the normal operation of the host --be it a bank, telecommunications carrier, or medical service provider -- we believe we have made a significant contribution towards assuring the reliability of the critical systems that the public relies upon on a daily basis. But greater satisfaction and success are achieved when a potentially devastating incident is <u>prevented</u> due to our prior involvement, participation, or sharing of information.

As a footnote, the Secret Service met recently with representatives of the Financial Services Information Sharing and Analysis Center (FS/ISAC) that was created pursuant to Presidential Decision Directive (PDD) 63. The directive mandated the Department of the Treasury to work with members of the banking and finance sector to enhance the security of the sector's information systems and other infrastructures, a responsibility managed by Treasury's Assistant Secretary of Financial Institutions. The role of the FS/ISAC is to devise a way to share information within the financial services industry relating to cyber threats and vulnerabilities. The Secret Service feels that it can make a significant contribution to the work of the FS/ISAC and is exploring common areas of interest with the FS/ISAC, to include information sharing.

The Secret Service continues to receive requests from local law enforcement agencies and others for assistance, and we welcome those requests. On an increasing basis, our local field offices and the Financial Crimes Division of the Secret Service receive desperate pleas from local police departments for physical assistance, training and equipment in the area of computer forensics and electronic crimes so that they can continue to provide a professional level of service and protection for their citizens. The Secret Service has become an important option for local law enforcement, the private sector and others to turn to when confronted with network intrusions and other sophisticated electronic crimes.

Over the past 3 years, Secret Service ECSAP agents completed 2,122 examinations on computer and telecommunications equipment. Although the Secret Service did not track the number of exams done for other law enforcement agencies during this period, it is estimated that some 10 to 15 percent of these examinations fell in this category. Many of the examinations were conducted in support of other agencies' investigations such as those involving child pornography or homicide cases simply because the requesting agency did not have the resources to complete the examination itself.

We do provide assistance on a regular basis to other departments, often sending ECSAP agents overnight to the requesting venue to perform computer related analyses or technical consultation. In fact, so critical was the need for even basic training in this regard that the Secret Service joined forces with the International Association of Chiefs of Police and the National Institute for Justice to create the "Best Practices Guide to Searching and Seizing Electronic Evidence" which is designed for the line officer and detective alike. Madam Chairman, with your permission, I would like to submit a copy of this guide for the record.

We have also worked with this group to produce the interactive, computer-based training program known as "Forward Edge" which takes the next step in training officers to conduct electronic crime investigations. Forward Edge incorporates virtual reality features as it presents three different investigative scenarios to the trainee. It also provides investigative options and technical support to develop the case. Copies of state computer crime laws for each of the fifty states as well as corresponding sample affidavits are also part of the two-CD training program and are immediately accessible for instant implementation.

Thus far we have dispensed over 220,000 “Best Practices Guides” to local and federal law enforcement officers and we will soon distribute, free of charge, over 20,000 Forward Edge training CDs.

In an additional effort to further enhance information sharing between the law enforcement community and the financial industry, the Secret Service recently created the “E Library” Internet website which serves as a mechanism for all members to post specific information, images and alerts relating to fictitious financial instruments, counterfeit checks, and credit card skimming devices. This website is accessible free of charge to all members of the law enforcement and banking communities and is the only such tool of its kind.

In today’s high tech criminal environment, the challenge to federal law enforcement and government is to identify existing repositories of expertise and provide a framework for inclusion and productive collaboration amongst the many government agencies and their respective industry and academic counterparts. The Secret Service is convinced that building trusted partnerships with the private sector and its Federal and local law enforcement partners is the model for combating electronic crimes in the information age.

Madam Chairman, that concludes my prepared statement, and I would be happy to answer any questions that you or other members of the subcommittee may have.